Claims

WHAT IS CLAIMED IS:

1. A computer program product encoding a computer program for executing a computer process on a mobile node, a network being coupled to a first base station and a second base station and the mobile node being fully authenticated by the first base station for fully authenticated access to the network, the computer process providing the mobile node with credential authenticated access to the network through the second base station prior to completion of full authentication of the mobile node by the second base station, the computer process comprising:

receiving at the mobile node a credential from the first base station, conditionally upon full authentication of the mobile node by the first base station;

transmitting from the mobile node an authentication message including the credential to the second base station to request credential authentication from the second base station; and

receiving credential authenticated access to the network for the mobile node through the second base station, if the second base station verifies the credential transmitted by the mobile node.

2. The computer program product of claim 1 wherein the computer process further comprises:

initiating a full authentication dialog with the second base station; and

completing the full authentication dialog with the second base station, responsive to the operation of receiving credential authenticated access to the network.

3. The computer program product of claim 1 wherein the credential is generated by the first base station.

4. The computer program product of claim 1 wherein the computer process further comprises:

receiving a challenge from the second base station; and

computing the authentication message based on an element of the challenge, wherein the operation of transmitting the authentication message is responsive to the operations of receiving the challenge and computing the authentication message.

5. The computer program of claim 1 wherein the computer process further comprises:

establishing a credential key cryptographically associated with the credential to prevent use of the credential without possession of the credential key.

6. The computer program product of claim 5 wherein the credential key is a secret key and the operation of computing the authentication message comprises:

computing a keyed one-way function based on the credential key and a challenge.

7. The computer program product of claim 5 wherein the credential key is a secret key encrypted into the credential.

8. The computer program product of claim 5 wherein the credential key is a secret key and the credential includes data for computing the credential key.

9. The computer program product of claim 5 wherein the credential key is a public key of a public-key cryptosystem and the credential includes data for authenticating the credential key.

10. The computer program product of claim 1 wherein the computer process further comprises:

determining a challenge time from a synchronized clock set; and

computing the authentication message based on the challenge time, wherein the operation of transmitting the authentication message is responsive to the operations of determining the challenge time and computing the authentication message.

11. The computer program product of claim 1 wherein the credential includes at least one trust parameter.

12. The computer program product of claim 1 wherein the first and second base stations share a shared key and the computer process further comprises:

authenticating the credential by cryptographic computation based on the shared key and data included in the credential.

13. The computer program product of claim 12 wherein the credential contains a received result of a keyed one-way function, and the authentication operation comprises:

computing a computed result of the keyed one-way function based on the shared key and the credential key; and

comparing the computed result with the received result.

14. The computer program product of claim 13 wherein the operation of computing a computed result of the keyed one-way function comprises:

computing a computed result of the keyed one-way function based on the shared key and the credential key, and at least one trust parameter.

15. The computer program product of claim 1 wherein the computer process further comprises:

establishing a credential key with the first base station, responsive to full authentication of the mobile node through the first base station, the credential key being associated with the credential.

16. The computer program product of claim 15 wherein the operation of establishing the credential key comprises:

receiving a secret credential key from the first base station via a secure communications link.

17. The computer program product of claim 15 wherein the operation of establishing the credential key comprising:

sending a public key of a public key cryptosystem to a first base station via an authenticated communication link.

18. In a network coupled to a first base station and a second base station and the mobile node being fully authenticated by the first base station for fully authenticated access to the network, a method for providing the mobile node with credential authenticated access to the network through the second base station prior to completion of full authentication of the mobile node by the second base station, the method comprising:

receiving at the mobile node a credential from the first base station, conditionally upon full authentication of the mobile node by the first base station;

transmitting from the mobile node an authentication message including the credential to the second base station to request credential authentication from the second base station; and

receiving credential authenticated access to the network for the mobile node through the second base station, if the second base station verifies the credential transmitted by the mobile node.

19. A mobile node capable of coupling to a network, the network being coupled to a first base station and a second base station and the mobile node being fully authenticated by the first base station for fully authenticated access to the network, the mobile node being capable of accessing with credential authenticated access to the network through the second base station prior to completion of full authentication of the mobile node by the second base station, the mobile node comprising:

a reception module receiving at the mobile node a credential from the first base station, conditionally upon full authentication of the mobile node by the first base station; and

a transmission module transmitting from the mobile node an authentication message including the credential to the second base station to request credential authentication from the second base station, wherein the reception module and the transmission module participate in credential authenticated access to the network for the mobile node through the second base station, if the second base station verifies the credential transmitted by the mobile node.

20. A computer program product encoding a computer program for executing a computer process on a mobile node, the computer process providing the mobile node with credential authenticated access to a network through a first base station after termination of fully authenticated access to the network through the first base station, the computer process comprising:

receiving a credential from the first base station, responsive to full authentication of the mobile node through the first base station;

detecting that fully authenticated access through the first base station has been terminated;

transmitting an authentication message including the credential to the first base station to request credential authentication from the first base station; and

receiving the credential authenticated access to the network through the first base station, if the first base station verifies the credential transmitted by the mobile node.

21. The computer program product of claim 20 wherein the computer process further comprises:

initiating a full authentication dialog with the first base station, responsive to the detecting operation; and

completing the full authentication dialog with the first base station, responsive to the operation of receiving the credential authenticated access to the network.

22. A method of providing a mobile node with credential authenticated access to a network through a first base station after termination of fully authenticated access to the network through the first base station, the method comprising:

receiving a credential from the first base station, responsive to full authentication of the mobile node through the first base station;

detecting that fully authenticated access through the first base station has been terminated;

transmitting an authentication message including the credential to the first base station to request credential authentication from the first base station; and

receiving the credential authenticated access to the network through the first base station, if the first base station verifies the credential transmitted by the mobile node.

23. A mobile node capable of establishing credential authenticated access to a network through a first base station after termination of fully authenticated access of the mobile node through the first base station, the mobile node comprising:

a reception module receiving a credential from the first base station, responsive to full authentication of the mobile node through the first base station;

a detector module detecting that fully authenticated access through the first base station has been terminated;

a transmission module transmitting an authentication message including the credential to the first base station to request credential authentication from the first base station, wherein the reception module and the transmission module participate in the credential authenticated access to the network through the first base station, if the first base station verifies the credential transmitted by the mobile node.

24. A computer program product encoding a computer program for executing a computer process on a computer system, a network being coupled to a first and a second base station, the computer process providing a mobile node with credential authenticated access to the network through the second base station prior to completion of full authentication of the mobile node through the second base station, the computer process comprising:

receiving a request for full authentication from the mobile node;

fully authenticating the mobile node to provide fully authenticated access the network; and

transmitting a credential to the mobile node, the credential including at least one trust parameter to allow the second base station to grant credential authenticated access to the network by the mobile node prior to completion of full authentication of the mobile node by the second base station.

25. The computer program product of claim 24 wherein the first and second base stations shared a shared key and the computer process further comprises:

encrypting a credential key and at least one trust parameter using the shared key to generate the credential.

26. The computer program product of claim 25 wherein the computer process further comprises:

computing an authentication code for the credential key and the at least one trust parameter using the shared key.

27. The computer program product of claim 24 wherein the first and second base stations share a shared key and the computer process further comprises:

encrypting a credential key, at least one trust parameter, and a keyed one-way function result based on the shared key to generate the credential, the keyed one-way function being a function of the credential key and the at least one trust parameter.

28. The computer program product of claim 24 wherein the first and second base stations share a shared key and the computer process further comprises:

generating a credential key from a keyed one-way function based on the shared key, the keyed one-way function being a function of a nonce.

29. The computer program product of claim 28 wherein the credential includes at least one trust parameter, the nonce, and the result of a keyed one-way function of the at least one trust parameter and the nonce, the keyed one-way function being based on the shared key.

30. The computer program product of claim 24 wherein the computer process further comprises:

transmitting a secret credential key to the mobile node via a secure communications link.

31. The computer program product of claim 24 wherein the computer process further comprises:

transmitting a public credential key to the mobile node via an authenticated communications link.

32. The computer program of claim 24 wherein the computer process further comprises:

cryptographically associating a credential key with the credential to prevent use of the credential without possession of the credential key.

33. The computer program product of claim 32 wherein the credential key is a secret key and the transmitting operation comprises:

computing a keyed one-way function based on a credential key and the challenge.

34. The computer program product of claim 33 wherein the credential key is a secret key and is encrypted into the credential.

35. The computer program product of claim 33 wherein the credential key is a public key and the credential includes data for computing the credential key.

36. The computer program product of claim 33 wherein the credential key is a public key of a public-key cryptosystem and the credential includes data for authenticating the credential key.

37. In a network coupled to a first and a second base station, a method of providing a mobile node with credential authenticated access to the network through the second base station prior to completion of full authentication of the mobile node through the second base station, the method comprising:

receiving a request for full authentication from the mobile node;

fully authenticating the mobile node to provide fully authenticated access the network; and

transmitting a credential to the mobile node, the credential allowing the second base station to grant credential authenticated access to the network by the mobile node prior to completion of full authentication of the mobile node by the second base station.

38. The method of claim 37 wherein the credential includes at least one trust parameter.

39. A first base station providing a mobile node with credential authenticated access to the network through the second base station prior to completion of full authentication of the mobile node through the second base station, the first base station comprising:

a reception module receiving a request for full authentication from the mobile node;

an authentication module fully authenticating the mobile node to provide fully authenticated access the network; and

a transmission module transmitting a credential to the mobile node, the credential allowing the second base station to grant credential authenticated access to the network by the mobile node prior to completion of full authentication of the mobile node by the second base station.

40. The first base station of claim 39 wherein the credential includes at least one trust parameter.

41. A computer program product encoding a computer program for executing a computer process on a computer system, wherein the network is coupled to a first and a second base station and the mobile node is fully authenticated by the first base station, the computer process for providing a mobile node with credential authenticated access to a network through a second base station prior to full authentication of the mobile node by the second base station, the mobile node having a credential received from the first base station responsive to full authentication by the first base station, the computer process comprising:

transmitting a challenge;

receiving an authentication message from the mobile node, responsive to the challenge, the authentication message including the credential to request credential authentication;

verifying the credential received from the mobile node; and

granting the mobile node with credential authenticated access to the network, if the credential transmitted by the mobile node is verified.

42. The computer program product of claim 41 wherein the computer process further comprises:

receiving a request for full authentication from the mobile node;

granting the request for full authentication responsive to the operations of granting the mobile node with credential authentication access to the network and receiving a request for full authentication.

43. The computer program product of claim 41 wherein the credential is generated by the first base station.

44. The computer program product of claim 41 wherein the first and second base stations share a shared key, and the verifying operation comprises:

decrypting the credential using the shared key; and

verifying an authentication code on the credential using the shared key.

45. The computer program product of claim 41 wherein the first and second base stations share a shared key, the challenge includes a challenge nonce, the authentication message includes a received keyed one-way function result and an encrypted credential key, and the verifying operation comprises:

decrypting the credential using the shared key;

computing a computed result of the keyed one-way function using the credential key and the challenge nonce; and

verifying the credential, if the computed result of the keyed one-way function matches the received keyed one-way function result.

46. The computer program product of claim 41 wherein the first and second base stations share a shared key, the challenge includes a challenge nonce, the authentication message includes at least one received trust parameter, a first received keyed one-way function result, a second received keyed one-way function result, a nonce of the first base station, and a credential key, and the verifying operation comprises:

computing a computed credential key using the shared key and the nonce of the first base station;

computing a first computed keyed one-way function result using the nonce of the first base station and the received trust parameters based on the shared key; and

trusting the computed credential key, if the first computed keyed one-way function result matches the first received keyed one-way function result.

47. The computer program product of claim 46 wherein, if the base station nonce is trusted, the verifying operation further comprises:

computing a second computed keyed one-way function result using the computed credential key and the challenge nonce; and

trusting the trust parameters, if the second computed keyed one-way function result matches the second received keyed one-way function result.

48. In a network coupled to a first base station and a second base station, a method of providing a mobile node with credential authenticated access to the network through the second base station prior to full authentication of the mobile node by the second base station, the mobile node having previously been fully authenticated by the first base station, the mobile node having a credential received from the first base station responsive to full authentication by the first base station, the method comprising:

transmitting a challenge;

receiving an authentication message from the mobile node, responsive to the challenge, the authentication message including the credential to request credential authentication;

verifying the credential received from the mobile node; and

granting the mobile node with credential authenticated access to the network, if the credential transmitted by the mobile node is verified.

49. An authenticating base station for providing a mobile node with credential authenticated access to a network through the authenticating base station prior to full authentication of the mobile node through the authenticating base station, the mobile node having a credential received from another base station responsive to being fully authenticated by the other base station, the authenticating base station comprising:

a transmission module transmitting a challenge;

a reception module receiving an authentication message from the mobile node, responsive to the challenge, the authentication message including the credential to request credential authentication; and

an authenticating module verifying the credential received from the mobile node and granting the mobile node with credential authenticated access to the network, if the credential transmitted by the mobile node is verified.